CONTRACTOR SYSTEM ACCESS, CONFIDENTIALITY, AND FERPA ADDENDUM

Laramie County Community College

This Addendum is incorporated into and made part of the agreement _____(the "Agreement") between Laramie County Community College ("LCCC") and _____ ("Contractor"). Except as modified by this Addendum, the Agreement remains in effect. If this Addendum conflicts with the Agreement regarding system access, confidentiality, privacy, security, or LCCC Data, this Addendum controls.

1. Definitions

"Authorized Personnel" means Contractor employees or approved subcontractor personnel who have a documented need for access to perform the Services and who are authorized in writing by LCCC.

"Education Records," "Personally Identifiable Information" or "PII," and "School Official" have the meanings assigned under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. Part 99 ("FERPA").

"LCCC Data" means all information, records, files, credentials, configurations, logs, and other data accessed, received, created, maintained, transmitted, or processed by Contractor for LCCC, including Education Records and PII.

"LCCC Systems" means LCCC-owned, licensed, hosted, or managed networks, applications, databases, devices, cloud environments, and related technology resources.

"Services" means the consulting, implementation, support, maintenance, assessment, project, or other professional services Contractor provides under the Agreement or an authorized statement of work or task order.

2. FERPA Status and Permitted Purpose

When the Services require access to Education Records without student consent, Contractor will act as a School Official performing an institutional service or function for which LCCC would otherwise use employees. Contractor will remain under LCCC's direct control with respect to the use and maintenance of Education Records.

Contractor may access, use, maintain, or disclose Education Records only to perform the specific Services authorized by LCCC and only for the purpose for which LCCC disclosed the information. Contractor will not use LCCC Data for Contractor's own purposes, advertising, marketing, profiling, product development, benchmarking, or any unrelated commercial purpose.

Contractor will comply with FERPA's restrictions on use and redisclosure, including 34 C.F.R. § 99.33, and with all other applicable privacy and confidentiality laws and LCCC policies communicated to Contractor.

3. Access Authorization and Least Privilege

Access is limited to Authorized Personnel and to the minimum systems, records, functions, and time period necessary for the assigned work. LCCC may approve, modify, suspend, or revoke access at any time.

Contractor will use only LCCC-issued or LCCC-approved accounts, devices, connection methods, repositories, and data-transfer methods. Credentials may not be shared. Multi-factor authentication must be used where required or made available by LCCC.

Contractor will not copy LCCC Data to personal devices, removable media, personal email, consumer file-sharing services, public code repositories, or any location not approved in writing by LCCC.

Access ends immediately when it is no longer required, when Authorized Personnel leave the engagement, or when the applicable task order or Agreement ends, whichever occurs first. Contractor will promptly notify LCCC when access should be removed.

4. Personnel, Training, and Conduct

Before receiving access, Authorized Personnel must complete any confidentiality acknowledgement, FERPA/privacy training, security awareness training, background check, or other onboarding requirement specified by LCCC.

Contractor is responsible for ensuring that Authorized Personnel understand and comply with this Addendum. Contractor will maintain a current list of Authorized Personnel and provide it to LCCC upon request.

Contractor will immediately notify LCCC of suspected misuse of access, policy violations, compromised credentials, or personnel changes affecting access.

5. Subcontractors and Third Parties

Contractor will not permit a subcontractor, affiliate, offshore resource, or other third party to access LCCC Systems or LCCC Data without LCCC's prior written approval.

Any approved subcontractor must be bound in writing to obligations at least as protective as those in this Addendum. Contractor remains responsible for the acts and omissions of its subcontractors and personnel.

LCCC Data may not be sold, shared, licensed, monetized, or disclosed to any third party except as expressly authorized in writing by LCCC or as required by law.

6. Security Safeguards

Contractor will implement reasonable and appropriate administrative, technical, and physical safeguards to protect LCCC Systems and LCCC Data against unauthorized access, acquisition, use, disclosure, alteration, loss, destruction, or unavailability.

At a minimum, Contractor will follow least-privilege access, secure credential practices, encryption in transit and at rest where Contractor stores or transmits LCCC Data, current security updates, malware protection, secure remote access, and logging appropriate to the Services.

Contractor will not disable, bypass, or interfere with LCCC security controls, monitoring, logging, backups, or change-management requirements. Security-sensitive or production changes require LCCC authorization and must be documented.

7. Security Incident Notification and Cooperation

Contractor will notify LCCC in writing without unreasonable delay and no later than twenty-four (24) hours after becoming aware of any actual or suspected unauthorized access to, acquisition of, use of, disclosure of, alteration of, loss of, destruction of, or inability to account for LCCC Data, or any compromise of credentials or LCCC Systems (a "Security Incident").

The notice will include, to the extent known, the nature and date of the Security Incident; systems, individuals, and data affected; actions taken to contain and mitigate it; and a contact for incident coordination. Contractor will preserve relevant evidence, cooperate with LCCC's investigation and response, provide updates, and not notify affected individuals or third parties on LCCC's behalf without LCCC's written authorization unless required by law.

8. Data Minimization, Retention, and Destruction

Contractor will access or receive only the LCCC Data reasonably necessary for the Services and will use de-identified or test data whenever LCCC determines it is sufficient.

Contractor will not retain LCCC Data longer than necessary for the Services or beyond an LCCC-approved retention period. Upon LCCC's written request, completion of the applicable work, or termination or expiration of the Agreement, Contractor will return or permanently destroy all LCCC Data in its possession, custody, or control, including copies, extracts, and local files, within ninety (90) days, unless a shorter period is required by LCCC or retention is required by law.

Destruction will be performed using an industry-recognized method appropriate to the media, such as NIST SP 800-88 or an equivalent standard. Upon request, Contractor will provide written certification of return or destruction. Data required by law to be retained remains subject to this Addendum and may not be used for any other purpose.

9. No Artificial Intelligence or Machine Learning Use

Contractor will not enter, upload, disclose, or use LCCC Data in a public or non-LCCC-approved artificial intelligence system. Contractor receives no right or license to use LCCC Data to train, tune, evaluate, benchmark, improve, develop, or operate any artificial intelligence or machine learning model, dataset, embedding, algorithm, analytics engine, or derivative product.

10. Records, Verification, and Compliance

Contractor will maintain records reasonably sufficient to demonstrate compliance with this Addendum, including Authorized Personnel, access approvals, training completion, approved data locations, and data return or destruction.

Upon reasonable request, Contractor will provide LCCC with documentation relevant to compliance and will cooperate with LCCC in responding to student requests, audits, investigations, legal process, or regulatory inquiries involving LCCC Data.

Contractor will promptly inform LCCC if it can no longer meet an obligation in this Addendum. LCCC may suspend access until the issue is resolved.

11. Remedies and Survival

A material violation of this Addendum constitutes a material breach of the Agreement. In addition to other available remedies, LCCC may immediately suspend Contractor access, require corrective action, or terminate the affected Services or Agreement as permitted by the Agreement and applicable law.

The obligations concerning confidentiality, permitted use, redisclosure, incident cooperation, return or destruction, and restrictions on artificial intelligence use survive expiration or termination for as long as Contractor retains or can access LCCC Data.

12. Ownership of Work Product and Intellectual Property

All deliverables, work product, software, source code, scripts, configurations, documentation, reports, designs, databases, workflows, integrations, and other materials created, developed, modified, or produced by Contractor for Laramie County Community College (“Work Product”) under the Agreement shall be the sole and exclusive property of LCCC.

Contractor hereby assigns and transfers to LCCC all right, title, and interest in and to such Work Product, including all associated intellectual property rights, upon creation.

Contractor shall not retain, reuse, sell, license, distribute, or otherwise exploit any Work Product developed for LCCC without LCCC's prior written authorization.

Upon request or termination of the Agreement, Contractor shall provide LCCC with all source code, compiled code, configuration files, documentation, credentials, architecture diagrams, and other materials necessary for LCCC to use, maintain, support, and modify the Work Product.

Contractor represents that the Work Product will not knowingly include proprietary materials of Contractor or third parties that would restrict LCCC's ownership or use of the Work Product unless specifically approved in writing by LCCC.

All code repositories created for LCCC shall reside in LCCC-owned repositories and organizational accounts. Contractor shall not maintain the authoritative copy of LCCC-developed code in personal or contractor-owned repositories.

Contractor shall maintain adequate documentation of work performed and, upon request, provide knowledge transfer sessions, documentation, diagrams, procedures, and operational instructions sufficient for LCCC personnel to maintain and support any systems or work product associated with the Services.

Contractor shall follow all LCCC change management, maintenance window, documentation, approval, testing, and rollback requirements.

Upon termination of access, Contractor shall return or destroy all credentials, certificates, tokens, encryption keys, VPN profiles, configuration backups, and copies of system documentation.

13. Security and Audit

Contractor acknowledges that activities performed within LCCC Systems may be monitored, logged, retained, and reviewed by LCCC for operational, security, compliance, and investigative purposes.

Contractor shall not create privileged accounts, service accounts, application accounts, administrative roles, security groups, or delegated permissions without written authorization from LCCC.

LCCC Data may not be accessed, processed, stored, transmitted, or replicated outside the United States without prior written approval from LCCC.

Contractor may not use LCCC contact information, directories, employee data, or student information for recruiting, marketing, solicitation, or commercial purposes.

Contractor shall not use AI-generated code, configuration, scripts, or content within LCCC environments unless specifically approved by LCCC and reviewed through established change management processes.

14. Governmental Sovereign Immunity

LCCC does not waive its sovereign immunity by entering into this Contract and specifically retains all immunities and defenses available to it as a governmental entity pursuant to the "Wyoming Governmental Claims Act", noted in Wyo. Stat. Ann. § 1-39-101, et seq., and all other applicable laws. LCCC fully retains all immunities and defenses provided by law with regard to any action, whether in tort, contract or any other theory of law, based on this Contract. Designations of venue, choice of law, enforcement actions, and similar provisions should not be construed as a waiver of sovereign immunity. The parties agree that any ambiguity in this Contract shall not be strictly construed, either against or for either party, except that any ambiguity as to sovereign immunity shall be construed in favor of sovereign immunity.

15. Indemnification

To the fullest extent permitted by law, Contractor agrees to indemnify and hold harmless LCCC, its elected and appointed officials, employees, officers, agents, successors, assignees and volunteers from any and all lawsuits, losses, liability for injuries, damages, claims, penalties, actions, demands or expenses arising from or in connection with work performed by or on behalf of Contractor for LCCC**.**